WHAT IS CLAIMED IS:

1. A common key exchanging method for exchanging a common key between two communication devices for transmission and reception of encrypted/authenticated data, comprising:

an information transmitting step, performed by at least one of the communication devices, of transmitting information required for another one of the communication devices to acquire the common key to the other one of the communication devices;

a setting step, performed by said at least one of the communication devices, of setting a waiting limit for a response from the other one of the communication devices based on a time required for a predetermined operation to be performed by the other one of the communication devices by a next response timing;

an acquiring step, performed by the other one of the communication devices, of acquiring the common key from the information by performing the predetermined operation; and

a response transmitting step, performed by the other one of the communication devices, of transmitting a predetermined response to the one of the communication devices in the next response timing.

2. The common key exchanging method according to claim 1, wherein

each of the communication devices calculates its own

public value for transmission to the other, and calculates the common key based on the public value received from the other, thereby achieving an exchange of the common key, and

in the setting step, the waiting limit is set based on at least either one of a time required for calculation of the public value performed by the other one of the communication devices and a time required for calculation of the common key performed by the other one of the communication devices.

3. The common key exchanging method according to claim 1, wherein

the one of the communication devices encrypts a common key generated by a unit included in the one of the communication devices or information for generating the common key and transmits the encrypted common key or the encrypted information, and the other of the communication devices decrypts the encrypted common key or the encrypted information to generate a common key and transmits a response of acknowledging the common key to the one of the communication devices, thereby achieving an exchange of the common key, and

in the setting step, the waiting limit is set based on a time required for decryption of the encrypted common key or a time required for decryption of the encrypted information and generation of the common key performed by the other one of the communication devices.

4. The common key exchanging method according to claim 1, wherein

after receiving a request message from the one of the communication devices, the other one of the communication devices encrypts the common key or information for generating a common key by using a public key received from the one of the communication devices and transmits the encrypted common key or the encrypted information to the one of the communication devices, thereby achieving an exchange of the common key, and

in the setting step, the waiting limit is set based on a time required for encryption of the common key or the information for generating the common key.

5. The common key exchanging method according to claim 1, wherein

the predetermined operation is either one of an operation for an authentication process associated with acquisition of the common key and an operation for acquisition of the common key and the authentication process accompanied thereby.

6. The common key exchanging method according to claim 5, wherein

the one of the communication devices transmits data with a digital signature for authentication to the other one of the

communication devices, and the other one of the communication devices performs an identity authentication process based on the data with the digital signature received from the one of the communication devices, thereby achieving the authentication process, and

in the setting step, the waiting limit is set based on a time required for the identity authentication process performed by the other one of the communication devices.

7. The common key exchanging method according to claim 5, wherein

the one of the communication devices transmits data using public key encryption for authentication to the other one of the communication devices, and the other one of the communication devices performs an identity authentication process based on the data using public key encryption received from the one of the communication devices, thereby achieving the authentication process, and

in the setting step, the waiting limit is set based on a time required for the identity authentication process performed by the other one of the communication devices.

8. The common key exchanging method according to claim 1, further comprising:

an estimating step, performed by the other one of the

communication devices, of estimating a required operation time to be taken for the predetermined operation;

a time transmitting step, performed by the other one of the communication devices, of transmitting the estimated required operation time to the one of the communication devices; and

a receiving step, performed by the one of the communication devices, of receiving the required operation time from the other one of the communication devices.

9. The common key exchanging method according to claim 8, further comprising

a step, performed by the one of the communication devices, of making an inquiry of the other one of the communication devices about the required operation time, wherein

in response to the inquiry from the one of the communication devices, the other one of the communication devices performs the estimating step and the time transmitting step.

10. The common key exchanging method according to claim 8, wherein

the other one of the communication devices stores in advance the required operation time.

11. The common key exchanging method according to

claim 1, further comprising:

a step, performed by the other one of the communication devices, of transmitting at least once to the one of the communication devices a report that a response will be delayed by the next response timing; and

a step, performed by the one of the communication devices, of receiving the report from the other one of the communication devices, wherein

in the setting step, a waiting limit for the response is set based on the report.

12. The common key exchanging method according to claim 1, further comprising:

a step, performed by the one of the communication devices, of measuring a time starting at a time of transmitting a message and ending at a time of receiving a response after the predetermined operation from the other one of the communication devices, so as to obtain a time to be taken for the predetermined operation.

13. The common key exchanging method according to claim 2, wherein

the public value and the common key are calculated by the other one of the communication devices by the next response timing, and

in the setting step, a waiting limit for a response with

regard to transmission of the public value or completion of calculation of the common key is calculated based on a total time to be taken for calculation of the public value and the common key performed by the other one of the communication devices.

14. The common key exchanging method according to claim 2, wherein

the public value is calculated by the other one of the communication devices by the next response timing, and

in the setting step, a waiting limit for a response with regard to transmission of the public value or completion of calculation of the common key is calculated based on a time to be taken for calculation of the public value performed by the other one of the communication devices.

15. The common key exchanging method according to claim 2, wherein

the common key is calculated by the other one of the communication devices by the next response timing, and

in the setting step, a waiting limit for a response with regard to transmission of the public value or completion of calculation of the common key is calculated based on a time to be taken for calculation of the common key performed by the other one of the communication devices.

16. The common key exchanging method according to claim 2, further comprising:

a step, performed by each one of the communication devices, of transmitting a completion report to the other after calculation of the common key has been completed; and

a step, performed by each one of the communication devices, of refraining from determining whether a key exchanging process has failed until a completion report is received from another one of the communication devices.

17. The common key exchanging method according to claim 2, wherein

the information transmitting step, the setting step, the acquiring step, and the response transmitting step are preformed in a message sequence in the IKE.

18. A communication device for exchanging a common key with a counterpart communication device for transmission and reception of encrypted/authenticated data, comprising:

an information transmitting section of transmitting information required for the counterpart communication device to acquire the common key to the counterpart communication device;

a receiving section for receiving a response from the counterpart communication device; and

a setting section for setting a waiting limit for the

response to be received by the receiving section from the counterpart communication device based on a time required for a predetermined operation to be performed by the counterpart communication device by a next response timing.

19. The communication device according to claim 18, further comprising:

an acquiring section for acquiring the common key from the information by performing the predetermined operation; and

a response transmitting section for transmitting a predetermined response to the counterpart communication device in the next response timing.

20. The communication device according to claim 18, wherein

the acquiring section includes:

a public value calculating section for calculating its own public value and transmitting the calculated public value to the counterpart communication device; and

a common key calculating section for calculating a common key based on a public key of the counterpart communication device received from the counterpart communication device, and

the setting section sets the waiting limit based on at least either one of a time required for calculation of the public value performed by the counterpart communication device and a time

required for calculation of the common key performed by the counterpart communication device.

21. The communication device according to claim 18, wherein

the acquiring section includes a common key calculating section for calculating the common key,

the information transmitting section performs a predetermined encryption process on the common key calculated by the common key calculating section or information for generating the common key for transmission to the counterpart communication device, and

the setting section sets the waiting limit based on either one of a time required for decryption of the encrypted common key performed by the counterpart communication device and a time required for decryption of the encrypted information and generation of the common key performed by the counterpart communication device.

22. The communication device according to claim 18, wherein

when the communication device receives either one of the common key which has been encrypted and information, which has been encrypted, for generating the common key from the counterpart communication device after transmitting an arbitrary

message, the setting section sets the waiting limit based on either one of a time required for encryption of the common key performed by the counterpart communication device and a time required for encryption of the information performed by the counterpart communication device.

23. The communication device according to claim 18, wherein

for transmission of data with a digital signature for authentication to the counterpart communication device, the setting section sets the waiting limit based on a time required for an identity authentication process performed by the counterpart communication device based on the data with the digital signature.

24. The communication device according to claim 18, wherein

for transmission of data using public key encryption for authentication to the counterpart communication device, the setting section sets the waiting limit based on a time required for an identity authentication process performed by the counterpart communication device based on the data using the public key encryption.

25. The communication device according to claim 18, wherein

the setting section obtains a time to be taken for the predetermined operation based on the required operation time estimated for the predetermined operation received from the counterpart communication device.

26. A communication device for exchanging a common key with a counterpart communication device for transmission and reception of encrypted/authenticated data, comprising:

a receiving section for receiving information required for obtaining the common key from the counterpart communication device;

a time transmitting section for transmitting information regarding a time required for obtaining the common key from the information received by the receiving section to the counterpart communication device;

an acquiring section for acquiring the common key from the information received by the receiving section by performing a predetermined operation; and

a response transmitting section for transmitting a predetermined response to the counterpart communication device in a predetermined response timing.

27. The communication device according to claim 26, further comprising:

an estimating section for estimating a required

operation time to be taken for a predetermined operation performed by a next response timing, wherein

the time transmitting section transmits the required operation time estimated by the estimating section to the counterpart communication device.

28. The communication device according to claim 19, further comprising:

an estimating section for estimating a required operation time to be taken for a predetermined operation performed by a next response timing,

a time transmitting section for transmitting the required operation time estimated by the estimating section to the counterpart communication device.

29. The communication device according to claim 18, further comprising

an inquiry transmitting section for making an inquiry of the counterpart communication device about the time required for the predetermined operation to be performed by the next response timing.

30. The communication device according to claim 19, further comprising

a delay report transmitting section for transmitting

a report that a response will be delayed to the counterpart communication device at least once by the next response timing.

31. The communication device according to claim 26, wherein

the time transmitting section transmits a report that a response will be delayed to the counterpart communication device at least once by the next response timing.

32. The communication device according to claim 18, wherein

the setting section measures a time starting at a time when a message is transmitted and ending at a time of receiving a response after the predetermined operation from the counterpart communication device.

33. A program for achieving a method of exchanging a common key for transmission and reception of encrypted/authenticated data between two communication devices, the program comprising:

an information transmitting step, performed by at least one of the communication devices, of transmitting information required for another one of the communication devices to acquire the common key to the other one of the communication devices;

a setting step, performed by said at least one of the

communication devices, of setting a waiting limit for a response from the other one of the communication devices based on a time required for a predetermined operation to be performed by the other one of the communication devices by a next response timing;

an acquiring step, performed by the other one of the communication devices, of acquiring the common key from the information by performing the predetermined operation; and

a response transmitting step, performed by the other one of the communication devices, of transmitting a predetermined response to the one of the communication devices in the next response timing.

34. A computer-readable recording medium having recorded thereon a program for achieving a method of exchanging a common key for transmission and reception of encrypted/authenticated data between two communication devices, the program comprising:

an information transmitting step, performed by at least one of the communication devices, of transmitting information required for another one of the communication devices to acquire the common key to the other one of the communication devices;

a setting step, performed by said at least one of the communication devices, of setting a waiting limit for a response from the other one of the communication devices based on a time required for a predetermined operation to be performed by the other

one of the communication devices by a next response timing;

an acquiring step, performed by the other one of the communication devices, of acquiring the common key from the information by performing the predetermined operation; and

a response transmitting step, performed by the other one of the communication devices, of transmitting a predetermined response to the one of the communication devices in the next response timing.